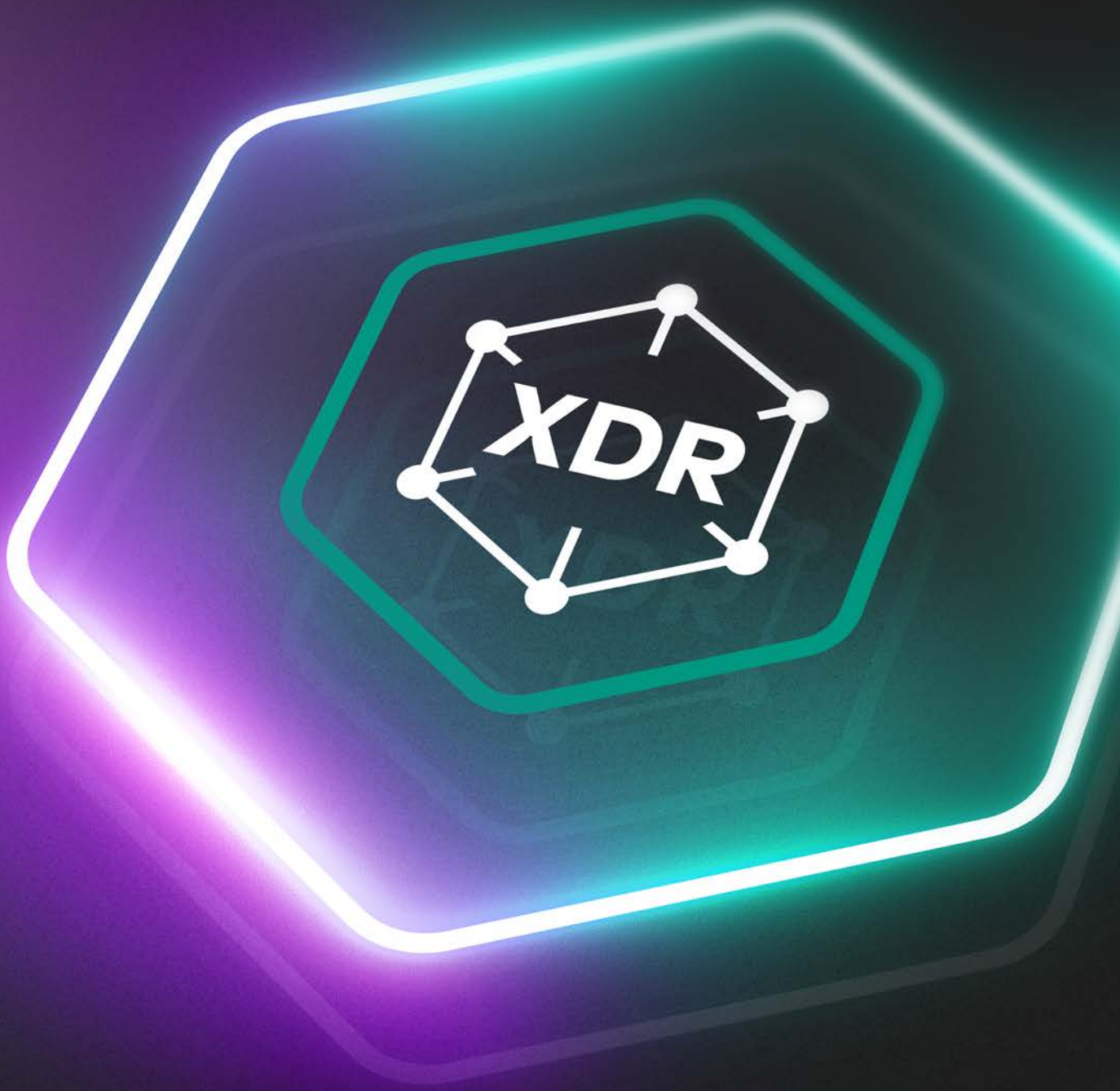


Informazioni senza confronti.
Protezione totale.

Kaspersky Extended Detection and Response

kaspersky BRING ON THE FUTURE

La complessità della cybersecurity delle aziende

Il panorama delle cyberminacce rende estremamente difficile per le organizzazioni stare al passo con la cybersecurity continuando a concentrarsi sulle operazioni aziendali fondamentali. Se a questo si aggiungono una superficie di attacco in continua espansione, requisiti normativi e il gap di competenze a livello globale, è facile capire perché le aziende moderne sono sotto pressione e perché così tanti attacchi informatici vanno a buon fine.

Il 51%

delle aziende ha difficoltà a rilevare le minacce avanzate e a condurre indagini con gli strumenti a disposizione

il 68%

delle aziende ha subito un attacco mirato alle proprie reti, con una perdita di dati come conseguenza diretta

6 trilioni di dollari

all'anno: il costo globale annuale del cybercrimine

400.000

nuovi malware vengono rilevati ogni giorno

Fonti: Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Extended Detection and Response

Visibilità completa. Protezione senza confronti.

Kaspersky XDR è un'efficiente soluzione di cybersecurity che garantisce la protezione dalle minacce informatiche sofisticate. Assicura un livello completo di visibilità, correlazione e automazione, sfruttando una vasta gamma di origini dati, inclusi dati di endpoint, rete e cloud.

Si è evoluto da Kaspersky Anti-Targeted Attack Platform come Native XDR nel 2016 e Open XDR nel 2023, fornendo una visione a 360° della sicurezza. Facilmente gestibile dalla Open Single Management Platform, Kaspersky XDR offre una sicurezza on-premises completa, garantendo che i dati sensibili dei clienti rimangano all'interno dell'infrastruttura e soddisfacendo al tempo stesso i requisiti di sovranità dei dati.

Open XDR

Le soluzioni Open XDR sono progettate per funzionare con un'ampia gamma di prodotti di sicurezza, consentendo alle organizzazioni di integrare le varie soluzioni di diversi fornitori, in modo da garantire maggiore flessibilità e funzionalità indipendenti dal vendor.

XDR nativo

Le soluzioni XDR native in genere funzionano perfettamente con l'ecosistema di strumenti di sicurezza del fornitore, fornendo un'esperienza più unificata e coesa. Queste soluzioni sono progettate appositamente per funzionare insieme, assicurando una completa integrazione, automazione e flussi di lavoro semplificati all'interno della suite di prodotti di sicurezza del fornitore.

Tecnologie chiave

Offriamo Open XDR come una singola piattaforma aperta, uno strumento universale per creare un ecosistema unificato di prodotti di cybersecurity. Al centro di Kaspersky XDR ci sono le nostre soluzioni leader: Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Endpoint Security for Business e Kaspersky Endpoint Detection and Response. Per la gestione avanzata della rete, KATA è un'opzione aggiuntiva.

Monitoraggio e analisi

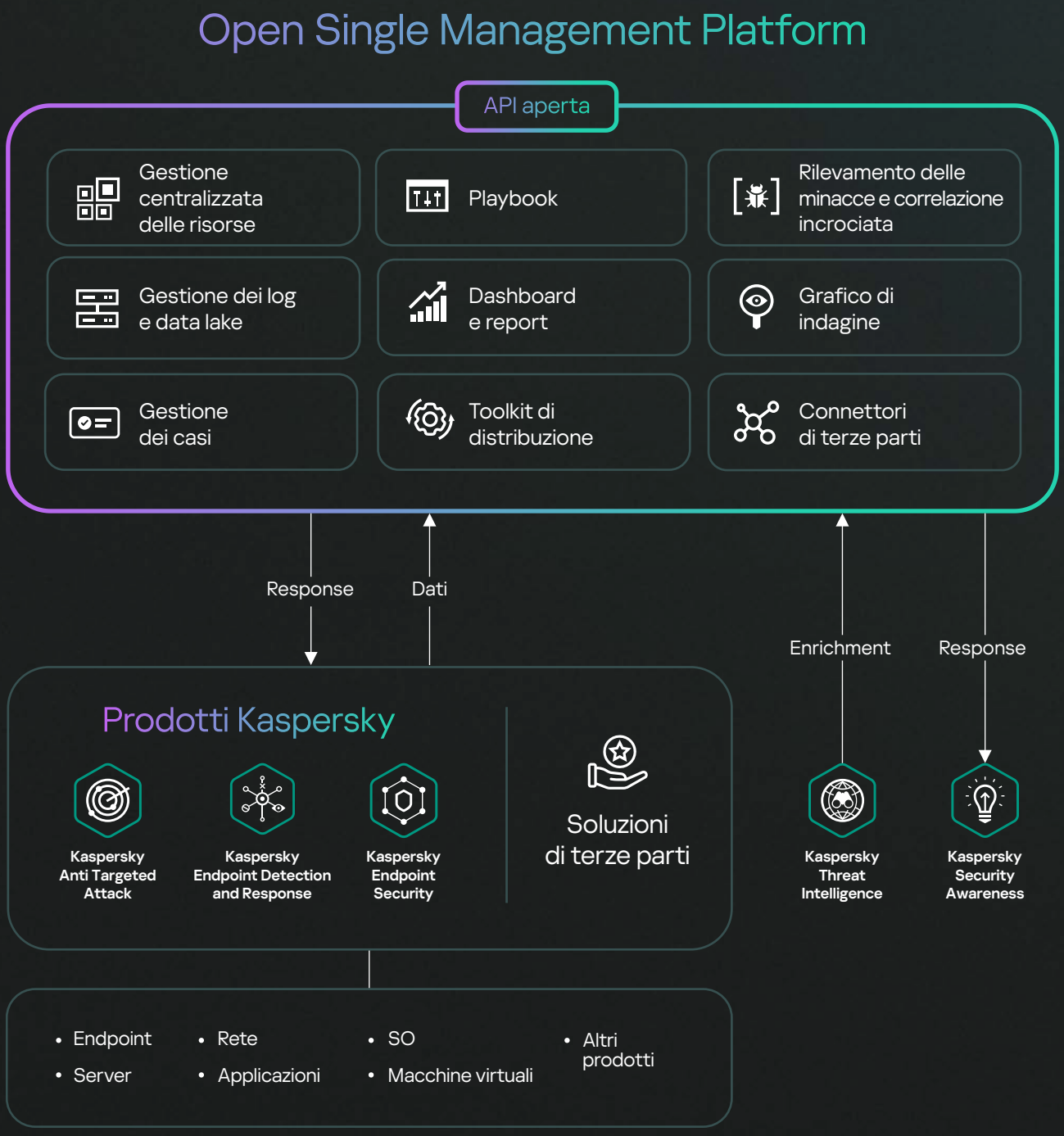
Fornisce raccolta e analisi centralizzate dei log, correlazione degli eventi di sicurezza in tempo reale e notifica tempestiva degli incidenti. Include un set pronto all'uso di regole di correlazione e l'accesso all'ampio portfolio di servizi Kaspersky Threat Intelligence per identificare e assegnare priorità a minacce, attacchi e IoC.

Protezione endpoint

Garantisce un'efficiente protezione degli endpoint da ransomware, malware e attacchi fileless. On-premises o nel cloud, la nostra protezione degli endpoint utilizza il machine learning e l'analisi del comportamento per proteggere tutti i tipi di endpoint che eseguono i principali sistemi operativi.

Endpoint Detection and Response

Offre una visibilità completa e protezioni superiori per tutti gli endpoint di un'organizzazione. La ricerca e l'individuazione delle minacce avanzate grazie all'esclusiva threat intelligence di Kaspersky, l'automazione delle attività di routine, i processi di indagine guidata e i rilevamenti personalizzabili promuovono una risoluzione rapida degli incidenti.



Funzionalità potenti, vantaggi significativi

Fusione dei dati in tempo reale da terze parti

La possibilità di integrare i dati da fonti di terze parti va oltre gli endpoint ed è ottimizzata dalla correlazione incrociata in tempo reale.

Risposta e remediation automatiche

Mettete in quarantena o isolate gli endpoint compromessi, bloccate le attività dannose e risolvete le vulnerabilità, riducendo le operazioni manuali e i tempi di risposta.

EPP/EDR all'avanguardia

Riconosciuta come azienda leader globale, Kaspersky rappresenta il punto di riferimento per le soluzioni EPP/EDR in tutto il mondo. Kaspersky EDR eccelle su scala globale, supportato da riconoscimenti e dalla partecipazione attiva a comitati internazionali come Interpol e MAPP.

Scalabilità senza confronti

In grado di supportare carichi che comprendono centinaia di migliaia di endpoint su una singola istanza, Kaspersky XDR tiene traccia con precisione delle minacce in tempo reale garantendo al tempo stesso un'elevata disponibilità.

Sovranità dei dati

Kaspersky è uno dei pochi fornitori che offre una soluzione XDR on-premises completa, garantendo che i dati sensibili dei clienti rimangano all'interno dell'infrastruttura e soddisfacendo i requisiti di sovranità dei dati.

Integrazione perfetta tra i prodotti Kaspersky

L'interazione tra i prodotti raggiunge un livello che rimane fuori dalla portata delle soluzioni di terze parti, grazie a un sistema di supporto unificato e un design perfettamente integrato.

Multi-tenancy per scenari MSSP

Fornite XDR come servizio con tenant completi: gli utenti di un tenant non possono vedere i dati degli altri tenant, mentre l'amministratore principale (MSSP) può creare processi di rilevamento e risposta per tutti i client.

Personalizzazione avanzata degli scenari di sicurezza e analisi dei dati a livello di infrastruttura

È possibile consentire agli utenti di configurare scenari di sicurezza complessi con la possibilità aggiuntiva di analizzare i dati nell'intera infrastruttura.

Funzionalità di integrazione

L'ampia gamma di integrazioni compatibili con Kaspersky XDR fornisce una visione unificata e contestualizzata delle potenziali minacce, fornendo al team di sicurezza tutti gli strumenti e le informazioni di cui ha bisogno per proteggere l'organizzazione da qualsiasi attacco sferrato dai cybercriminali.

Le funzionalità di integrazione del prodotto comprendono la capacità di ricevere dati (log) da altri sistemi e dispositivi, nonché di impostare risposte automatizzate in altri prodotti. Kaspersky XDR include un'ampia gamma di integrazioni pronte all'uso, con prodotti Kaspersky e di terze parti. È anche possibile aggiungere ulteriori integrazioni che possono essere sviluppate da Kaspersky Professional Services, dai partner o dai clienti stessi (incluso l'utilizzo delle funzionalità API dei prodotti collegabili). È possibile l'integrazione con sistemi di vari domini e fornitori diversi e sono supportati numerosi protocolli e formati di dati.

Per dominio di sicurezza

Endpoint Security

- Soluzioni EDR ed EPP

Sicurezza di rete, Web ed e-mail

- Protezione e-mail
- Network Detection and Response (NDR)
- Firewall (FW) e firewall di nuova generazione (NGFW)
- Gestione unificata delle minacce (UTM)
- Sistemi di rilevamento delle intrusioni (IDS)

Cloud Security

- CASB (Cloud Access Security Broker)
- CWPP (Cloud Workload Protection Platform)

Threat intelligence

- Cyber Threat Intelligence (CTI)

Sicurezza dell'identità

- Identity and Access Management (IAM)
- Privileged Access Management (PAM)

Security Awareness per OT/IoT

Per tipo di trasporto

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- File
- 1c-log e 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

Per tipo di dati

- XML
- SysLog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

Per vendor

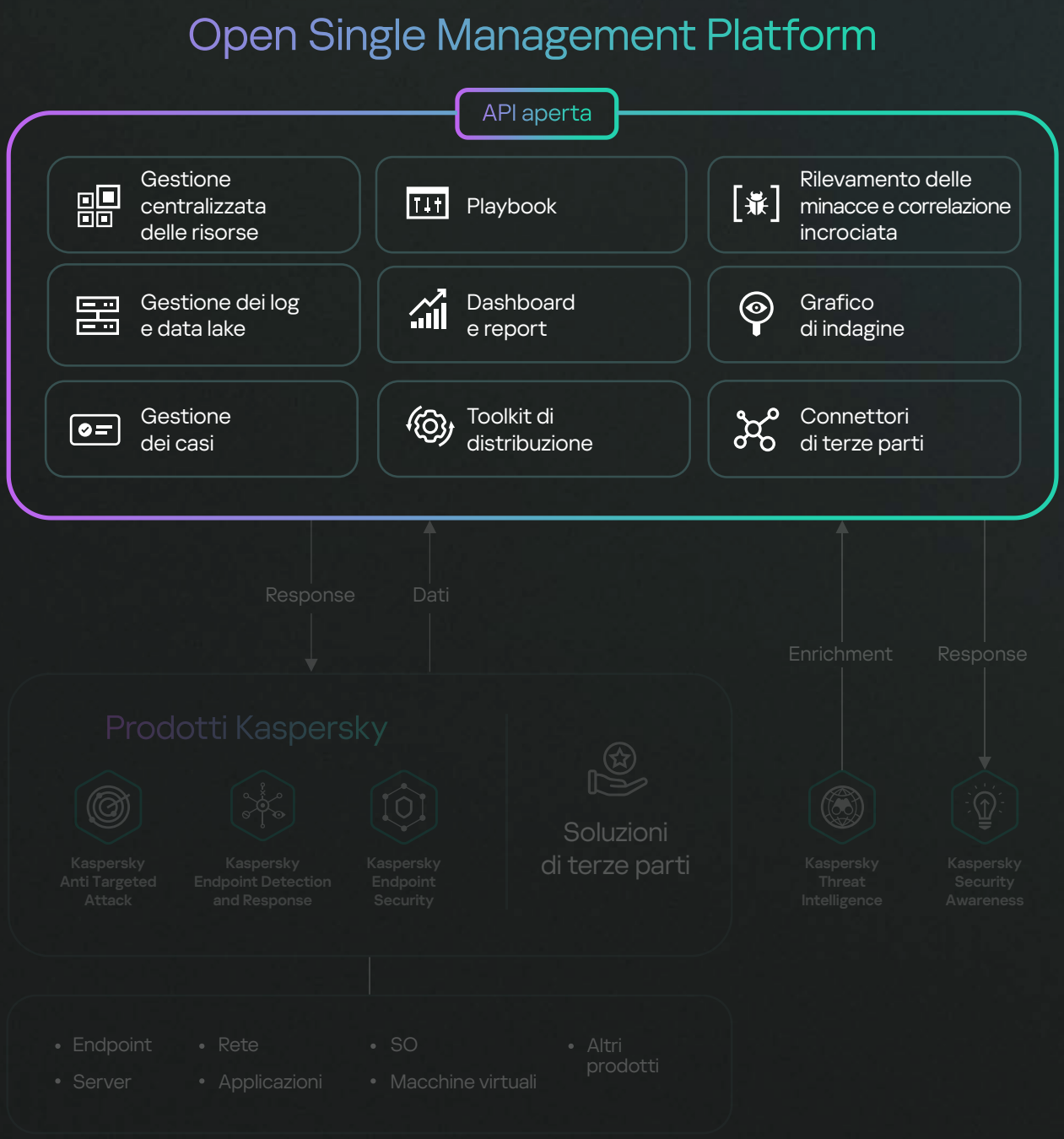
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard - Firebox
- Winchill Fracas
- Zettaset
- Zscaler & etc.

Cosa offriamo

Kaspersky XDR è disponibile in due opzioni.

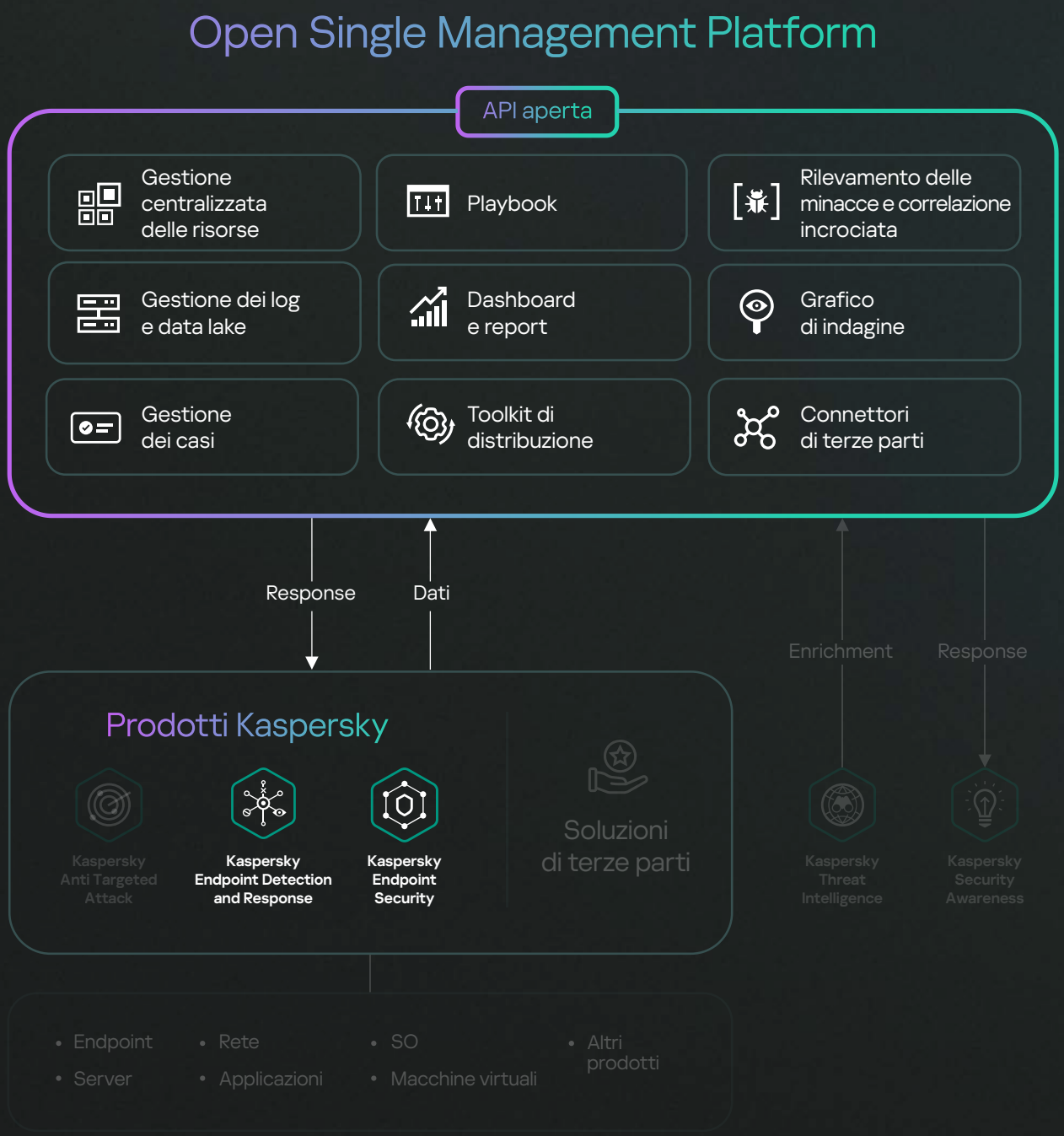
KasperskyXDR Core

Kaspersky XDR Core è rivolto ai clienti che dispongono già di soluzioni endpoint ed EDR e non desiderano sostituirle, ma preferiscono estendere la funzionalità con un motore di correlazione, risposte automatizzate e connettori di terze parti.



Kaspersky XDR Expert

Kaspersky XDR Expert combina la migliore protezione degli endpoint con le funzionalità di rilevamento avanzate di Kaspersky EDR Expert, un motore di correlazione e risposte automatizzate. È possibile aggiungere connettori di terze parti per riunire tutti i dati.



Valore aggiunto con sensori supplementari

Kaspersky XDR supporta l'integrazione di sensori supplementari progettati per proteggere risorse specifiche, integrandosi perfettamente in XDR per fornire ancora più valore e trasformando XDR in una piattaforma coesa che offre agli analisti uno spazio di lavoro centralizzato che abbraccia tutte le soluzioni integrate.

Kaspersky XDR non solo potenzia le vostre difese tramite EDR, ma offre anche funzionalità di integrazione flessibili, in modo che i clienti possano aggiungere prodotti all'ecosistema in qualsiasi momento.

		Kaspersky XDR Core	Kaspersky XDR Expert
Open Single Management Platform e relativi componenti	Motore di correlazione incrociata (fornito da KUMA) • Connettori di terze parti • Gestione dei log e data lake • Rilevamento delle minacce e correlazione incrociata • Gestione delle risorse • Dashboard e report	●	●
	Componenti XDR • Gestione dei casi • Orchestrazione e automazione della risposta (playbook) • Investigation • Toolkit di distribuzione • API aperta	●	●
Kaspersky EDR e funzionalità KESB	Rilevamento manuale, semi-automatizzato e automatizzato		●
	Monitoraggio tra endpoint protetti		●
	Contenimento minaccia		●
	Opzioni di ripristino		●

Kaspersky XDR Core

Kaspersky Unified Monitoring and Analysis Platform

Componenti XDR

Kaspersky XDR Expert

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Business

Kaspersky Endpoint Detection and Response

Componenti XDR

Perché Kaspersky XDR

La più testata. La più premiata. Protezione Kaspersky.

Kaspersky è un'affermata azienda globale di cybersecurity con una solida esperienza in materia di sicurezza. Proteggiamo organizzazioni in tutto il mondo da oltre 25 anni e abbiamo ricevuto innumerevoli premi e riconoscimenti per i nostri prodotti e servizi. Tra il 2013 e il 2022, i prodotti Kaspersky:

827

hanno partecipato a 827 test e recensioni indipendenti

587

si sono classificati 587 volte al primo posto

685

si sono classificati 685 volte nelle prime tre posizioni

Nel 2023, Kaspersky è stata nominata Leader nel mercato delle soluzioni XDR dall'autorevole società di consulenza e ricerca tecnologica globale ISG. ISG definisce "leader" coloro che dispongono di un'offerta completa di prodotti e servizi e rappresentano la forza innovativa e la stabilità competitiva.

Per saperne di più

Kaspersky Extended Detection and Response

Richiesta demo

www.kaspersky.it

© 2023 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.

#kaspersky
#bringonthefuture